

# STAFF SUMMARY SHEET

	TO	ACTION	SIGNATURE (Surname), GRADE AND DATE		TO	ACTION	SIGNATURE (Surname), GRADE AND DATE
1	Dept Rsrch Director	coord	<i>Carl AD 24 27 Feb 14</i> MARTIN C. CARLISLE, AD-24	6			
2	DFCS	sig	<i>Gregory Schechtman AD 24 27 Feb 14</i> GREGORY SCHECHTMAN, COL	7			
3	DFER	approve	<i>Salte, AD-22, 29 Feb 14</i>	8			
4	DFCS	action	DAVID J. CASWELL, MAJ	9			
5				10			

SURNAME OF ACTION OFFICER AND GRADE  
Caswell, O-4

SYMBOL  
DFCS

PHONE  
333-6803

TYPIST'S  
INITIALS  
djg

SUSPENSE DATE  
20140307

SUBJECT  
Clearance for Material for Public Release

USAFA-DF-PA- 146

DATE  
20140228

## SUMMARY

1. PURPOSE. To provide security and policy review on the document at Tab 1 prior to release to the public.

## 2. BACKGROUND.

Authors: Maj David Caswell, Capt Eric Dowty, Capt Jason McGinthy

Title: Supervisory Control and Data Acquisition Security Awareness in a Resource Constrained Learning Environment

Circle one: Abstract    Tech Report    Journal Article    Speech    Paper    Presentation    Poster  
Thesis/Dissertation    Book    Other: \_\_\_\_\_

Check all that apply (For Communications Purposes):

☐ CRADA (Cooperative Research and Development Agreement) exists

☐ Photo/ Video Opportunities    ☐ STEM-outreach Related    ☐ New Invention/ Discovery/ Patent

Description: Paper for 18th Colloquium for Information Systems Security Education

Release Information:

Previous Clearance information: (If applicable) N/A

Recommended Distribution Statement: Distribution A: approved for public release, distribution unlimited

3. DISCUSSION. The material is based on ongoing work to create an interactive teaching tool for highlighting cyber threats. The Department Research Director has reviewed this poster and recommends it for public release

4. RECOMMENDATION. Sign Coord block above indicating document is suitable for public release. Suitability is based solely on the document being unclassified, not jeopardizing DoD interest, and accurately portraying official policy.

*David J. Caswell*  
DAVID J. CASWELL, Maj, USAF  
Assistant Professor

1 Tab: Tab 1) Paper for Approval

# **Supervisory Control and Data Acquisition (SCADA) Security Awareness In a Resource Constrained Learning Environment**

David J. Caswell, Eric M. Dowty, Jason M McGinthy, *United States Air Force Academy*

**Abstract** – *SCADA security is a terrific educational topic to highlight the threats and vulnerabilities that exist in the information technology arena for all (technical and non-technical) students. Further, using inexpensive parts, schools can construct an interactive model that allows students to experience SCADA attacks from both the position of the target and the attacker. This experience can be used to highlight several useful lessons that reinforce the need for security mindedness in all professions. In this paper we describe the design and construction of both the physical and logical aspects of our SCADA city and how it is used for the computer science 0.5 course.*

**Keywords** – Information Assurance, Education, SCADA, ICS, model

## **I. INTRODUCTION**

Vulnerabilities of SCADA systems and the subsequent threat to critical infrastructure and industry are not new topics in Information System (IS) security education. Neither is the high-level of threat that these vulnerabilities present in the physical domain. In remarks during a 2012 meeting of the Business Executives for National Security, then Secretary of Defense Leon Panetta stated “a cyber-attack perpetrated by nation states or extremist groups could be as destructive as the terrorist attack on 9/11” [1]. Given the threat level, coupled with the reality that most SCADA systems are connected in some manner to the Global Information Grid (GIG), the requirement to educate future computer scientists, software

developers, and leaders in IS security in this area is more important than ever.

The ability to educate students about these vulnerabilities beyond simply lecture and case study is difficult. Creating a lab-like environment where students can interact with an Industrial Control System (ICS) and Programmable Logic Controllers (PLCs) can be cost prohibitive and/or exceedingly complex. Further, the ability to empower students to actually demonstrate real world effects in a SCADA environment becomes even more costly and complex. This paper discusses how to create a cost effective, technically streamlined, physical SCADA environment to raise security awareness for students and educators alike. For the purpose of readability, we will refer to the set of vulnerabilities and attacks that target SCADA or ICS systems simply as SCADA attacks or vulnerabilities.

### *A. Spectrum of SCADA Vulnerabilities*

The threat to SCADA systems was recently highlighted in a 2013 report to the U.S. House of Representatives detailing the significant vulnerability to the electric grid’s control systems [2]. However, SCADA vulnerabilities extend well beyond the power grid. The United States’ Presidential Policy Directive 21 (PPD-21), *Critical Infrastructure Security and Resilience*, identifies 16 critical infrastructure sectors that must be strengthened against both physical and cyber-attack [3]. Many of these sectors rely heavily on SCADA systems including, but not limited to: Critical Manufacturing, Dams, Energy, Nuclear Reactors, Materials, and Waste, Transportation Systems, Water and Wastewater Systems.

Primary effects from a SCADA attack typically result from altering or shutting down the targeted system. Perhaps the most notable example is the manipulation of centrifuges at the Natanz uranium enrichment facility by the STUXNET worm [4]. In this attack, the worm not only changed the speed of the centrifuges but also provided fake data to the human controllers to make the system appear to be functioning normally. A possible extension of STUXNET would be to attempt to have the centrifuges self-destruct by overspinning or moving out of phase similar to what was demonstrated in the 2006 AURORA test [5].

These primary effects, however, are only the first element of concern from a SCADA attack. Due to the prevalence of SCADA systems, any attack on them can have far reaching secondary or tertiary effects, many that may be direr than the initiating attack. A simple example is the impact of shutting down a power substation that is the primary source of power for a hospital.

#### *B. Who needs SCADA Security Awareness*

As SCADA attacks are threats against information systems, it is easy to say that future computer scientists, software developers, and leaders in IS security need to be aware of the implications to critical infrastructure. With this awareness they can be charged with the design, construction, security, and maintenance of legacy and future SCADA systems.

We, however, think that focusing on IT professionals is too small a subset for this topic and that a wider range of students including engineers, chemists, biologists, operations managers, etc. should be aware of the vulnerabilities inherent in SCADA systems. There is a high likelihood that the students of today will have careers that deal with SCADA systems. Even those who do not directly choose to focus on information technology will be directly supported by SCADA systems. These professionals should be aware of the vulnerabilities so they can take intelligent precautions to mitigate attacks. SCADA system vulnerabilities are not going to be a quick fix; as educators we must play the long game in helping to develop this expertise.

To this end, lectures and case studies in SCADA vulnerabilities are very useful. However, creating a hands-on experience for students to secure, defend, and attack SCADA systems with realistic sequences of consequences creates an invaluable learning opportunity. The use of the highly interactive activity improves retention and understanding of the learning outcomes [6]. Due to the impact these vulnerabilities can have on the economy, military, and our way of life, it is imperative that educators make lessons as powerful, substantive, and memorable as possible all of the while working within the constrained timing typically available in the curricula. This particular topic is typically a footnote in the entirety of a Computer Science curriculum, so it is imperative that educators make lessons in SCADA vulnerabilities really count.

## II. INTERACTIVE SCADA ATTACK EDUCATION

### *A. Student Outcomes*

If the topic of SCADA vulnerabilities is taught as part of a core curriculum introduction to computer science course, e.g. Computer Science 0.5, then it is essential that the material be taught so that it is accessible to a variety of backgrounds to include engineers, chemists, biologists, management, political scientists and others whose jobs will involve working with SCADA systems. We have found that this is a perfect opportunity to present the implications of SCADA attacks so that all students leave the course with an appreciation of the threat.

As the initial introduction to SCADA is intended to be for all students, including both those focusing on IT and those with other preferences, our student outcomes are purposefully broad. When designing this lesson we focused the learning outcomes on the primary and secondary effects of SCADA attacks and limited the technical depth we expected of the students. To this end, our educational outcomes are:

- Appreciate the breadth of systems potentially vulnerable to SCADA attacks
- Identify realistic effects directly resulting from a SCADA attack

- Understand secondary and tertiary effects resulting from an attack on SCADA system(s)
- Identify the risks of a system to different types of SCADA attacks
- Describe common causes of SCADA vulnerabilities
- Describe mitigation options for protecting a system from SCADA attacks

For students that go on to pursue a degree in Computer Science or related disciplines this introduction provides a spring board that encourages students to think about security as they progress through their major's courses. Using the litany of effects that could result from a SCADA attack provides numerous examples that later courses can leverage for ensuring a security by design mentality for these future IT professionals. Some educational outcomes for these higher level courses include:

- Evaluate ICS protocol and identify vulnerabilities for the SCADA receiver
- Develop approaches to protect a SCADA system from specific types of attacks
- Assess the risk of a SCADA attack being successful against a targeted systems
- Implement protection methods for defending a particular system from SCADA attacks

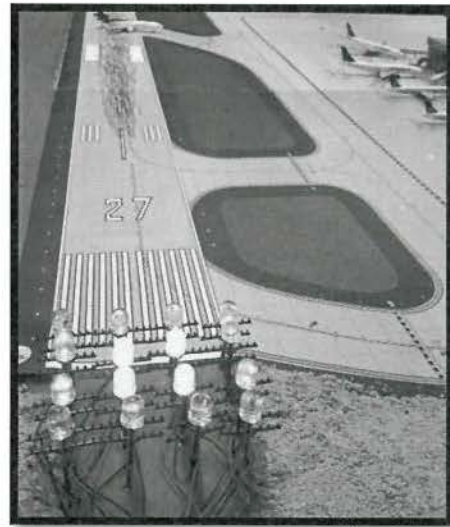
For students who do not remain in the IT realm, this introduction provides an awareness to help them mitigate threats for their chosen domain.

To solidify the student appreciation of SCADA vulnerabilities we have developed an automated model city dubbed *CyberVille*. We constructed CyberVille using scale models of a variety of commercial, industrial, and residential facilities with a model train set and programmable light and motion controllers. Similar to the professional Cyber City from SANS [7], CyberVille provides an interactive city to study SCADA attacks. Unlike SANS Cyber City, the total cost of CyberVille is well under \$10K and is completely customizable to support the level of interaction needed for the level and understanding of the students being taught. Compared to developing a SCADA

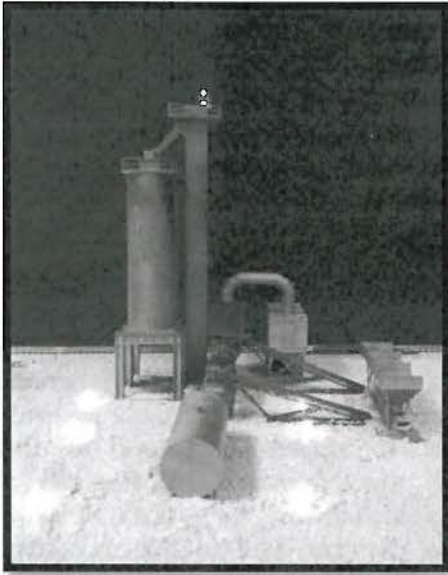
environment using ICS software, PLCs, and motor generators or other pieces of automated hardware, this approach keeps the cost and maintenance of both the software and hardware to a minimum while still creating an interactive and engaging environment for our students.

### B. *CyberVille*

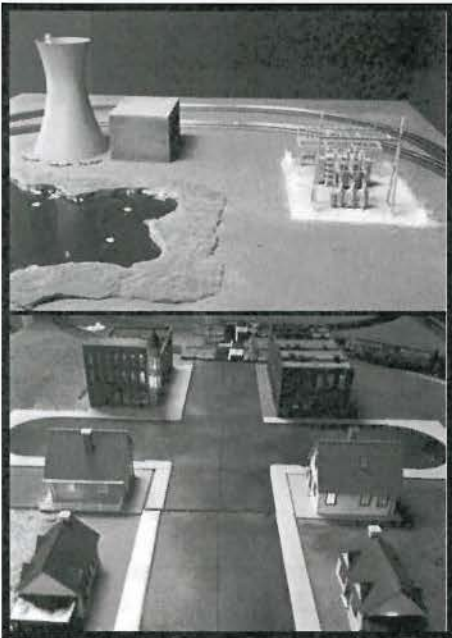
CyberVille consists of two four foot by eight foot tables supporting the models on top and the wiring underneath. Several SCADA-like systems are automated using the programmable lights and motors. Each of these systems were designed to support some level of direct or indirect effect from a SCADA attack. These systems include an Air Traffic Control and Landing System (ATCALS), manufacturing plant, railroad control, water treatment facility, nuclear power plant, power substation, and fuel storage. Figure 1 through 6 depict each of these facilities and describes the SCADA effect that can be controlled for the students.



**Figure 1: Air Traffic Control and Landing System (ATCALS).** Students can control the direction, power, and speed of the lights. Along with other aircraft landing lights, this represents an attack on the aircraft landing navigation systems used at airports.

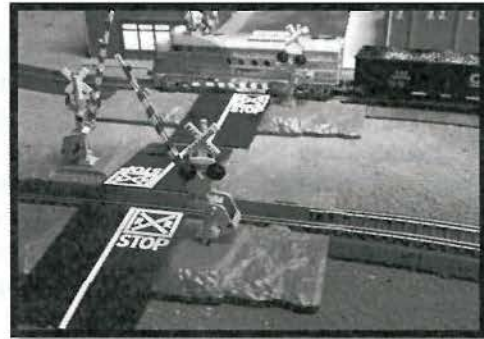


**Figure 2: Manufacturing Plant.** Students can control the power to the plant. This represents a direct attack against a target..



**Figure 3: Power Plant, Transmission, City Lights.** Students can control the power from the plant or the substation (shown by the building lights flickering, toggling, etc.), the

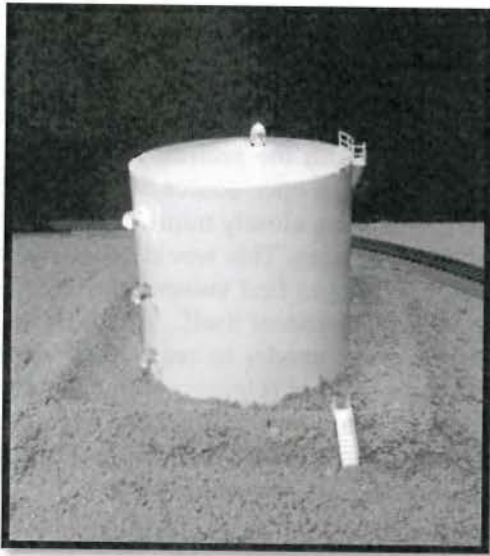
stability of the plant (represented by status lights moving from red to blue), or the transmission (shown by lights moving on telephone poles towards the city). This represents attacks on the different components of power transmission including the power plant, substation, and residential or commercial facilities.



**Figure 4: Railroad Track Control, Railroad Crossings.** Students can control the train speed and direction as well as the track toggling. This represents an attack on the transportation infrastructure.

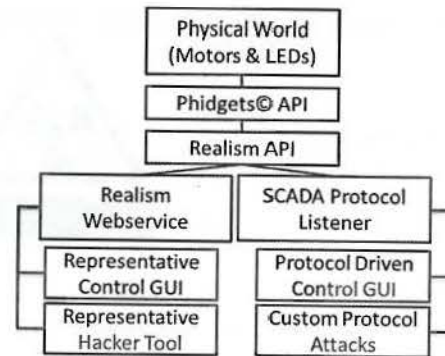


**Figure 5: Water Treatment Facility, Water Delivery.** Students can contaminate the water (as shown by lights that change from blue to red underneath a plasticized water). This represents an attack on fresh water infrastructure.



**Figure 6: Fuel Storage.** Students can contaminate the fuel (as shown by color indicators on the storage unit). This represents an attack on transportation network as contaminated fuel for an aircraft jet engine could cause catastrophic engine failure.

Our overall design approach starts with the physical models and the requisite LED or servos to visually display the effects of an attack. Next we connect the LEDs and motors through a USB API to what we call our realism API. In this API we synchronize the motors and lights to replicate what would occur in the system under normal operations and during an attack. This API then connects to web-service that allows external control by in-house built tools. Our long-term plan is to also connect a SCADA protocol receiver to this realism API to have CyberVille respond to real protocols instead of just the direct commands of the web service. Figure 7 depicts these connections.



**Figure 7: High Level Communication Design**

To control the model's automated lights and motors we used components known as Phidgets© (available at [www.phidgets.com](http://www.phidgets.com)). These components provided us low cost USB sensing and control devices, which can be custom programmed to a specific purpose through the Phidgets API. Phidgets offer a number of sensors and controls, however, for the purpose of CyberVille, we primarily used their LEDs, servos, and associated controllers.

Since we built the webservice to communicate with the realism API, the students are able to interact with the town in both of the roles of the standard user and as an attacker. This allows students to easily gain a sense of how the attack would work (at the highest level) without having to understand the underlying protocols, system vulnerabilities, etc. This same connectivity also lets us put together realistic user control software to emulate what a non-attacker would see/operate on (ICS) for the SCADA system.

An example of the realism API is the power plant ICS shown in Figure 8. This controls the power plant production and transmission for the city, which mimics (in a simplified manner) power production and transmission for CyberVille.



**Figure 8: Power Plant ICS**

An attacker can make use of the realism API as well by sending a series of command line attacks to interfere with the power plant operator. These attacks are only limited by the programmer's ability to implement. In its current form we have primarily focused on the power system where our programmed attacks include:

- Lowering power production causing brownout in CyberVille
- Halting power production causing black out in CyberVille
- Blinding the operator to the loss of power production so all seems nominal

This can be a powerful tool for demonstrating various implications of SCADA attacks to students. Together the attacker and non-attacker interfaces let students gain a sense of what both sides of the attack would experience. In the future, we hope that allowing the students to develop their own attacks will further enhance student understanding of the limits and consequences of SCADA vulnerabilities.



**Figure 9: Attacker Command Line**

Our next step for this development is to build a SCADA protocol listener that would communicate with the realism API. With this we could leverage open-source SCADA protocol emulators to more closely mimic the interactions of SCADA devices. This would allow advanced student attackers to find vulnerabilities and craft exploits in the protocol itself. This addition will let us adapt the model to respond to whatever protocol we feel has relevance to the students. It will also create a more robust attacker/defender experience to develop plausible solutions for mitigating SCADA vulnerabilities.

### C. Top-Down Education Approach

Rather than educating students on SCADA vulnerabilities from the bottom-up as may be expected, we recommend using a top-down approach. In this approach the educator first presents the high level of a SCADA attack. This discussion can be tailored to the student audience. For example, the military and political implications of the STUXNET attack being a catalyst for nation state actors to condone and invest in more cyber weapons of this caliber. Educators could also have their classes hypothesize on other strategic implications such as what impact a persistent blackout would have on local and national economies.

Once a firm understanding of the strategic impacts has been gained, the operational level of a SCADA attack should be taught. At this level students can be asked to start thinking about what “end-game” effect could be used to achieve a stated objective followed by designing an attack vector. Using CyberVille we ask our students to consider different “end-game” scenarios, such as halting manufacturing at the manufacturing plant (Figure 2). The students are allowed to examine all the different SCADA systems which supply some level of service to the plant, such as power, water supply, water treatment, transportation, etc. They can then identify what SCADA attack vector they would like to pursue in CyberVille. This could be an attack on power generation, power transmission, disrupting water supplies/treatment,

transportation of goods to and from the plant, or any other attack vector they can come up with.

After they identify what target would be attacked they have to discuss the ramifications of the attack. These ramifications include not only what would be the immediate effect but also the indirect effects. These indirect effects could include how long the results of the attack would persist and what other groups would be effected by the attack. Once they have identified the implications of the attack they can then switch to examining the actual attack itself at a more tactical level.

At the tactical level the students can now start to interact with CyberVille directly. In future iterations of CyberVille, students in higher level courses will be able to perform reconnaissance and scan the ICS systems of CyberVille to identify penetration points as well as identify vulnerabilities in the ICS protocols. Currently, students are limited to the vulnerabilities and exploits developed by the faculty based on the realism APIs web service. Once vulnerabilities and exploits have been identified the students attack CyberVille SCADA systems through the cyber domain and watch their exploits play out in real time in the physical models of CyberVille.

All of the discussion on SCADA attacks is focused on promoting awareness of the vulnerabilities and an understanding of actions needed to defend against the vulnerabilities. Once students are able to understand how attacks occur they can then be charged with developing and implementing defenses. Understanding how and why to implement these defenses is the primary purpose of this approach.



**Figure 13: SCADA Education Pyramid**

#### *D. Future Iterations of CyberVille*

CyberVille is an ever expanding project, with the only limits being the imagination of our students and faculty. In our curriculum it is currently used in the freshman level Computer Science survey course. However, it is being expanded for use in our Science, Technology, Engineering, and Mathematics (STEM) outreach programs as well as integration into higher level courses, where students will be able to plan and execute their own attacks on ICS' using the SCADA protocol emulator.

Development is currently on-going to both expand the realism API as well as to create the SCADA protocol emulator. The emulator will simulate real-world equivalent SCADA protocols, link them to Phidgets actions in the CyberVille model, and enable more realistic ICS representations for non-attackers to control the CyberVille SCADA systems.

#### *E. Developing Your Own CyberVille*

CyberVille does not have to be as extensive as the one discussed in this paper. The development of a single SCADA system with a physical model, controlled by Phidgets, linked to the cyber domain through a realism API is enough for students to experience the effects of SCADA vulnerabilities and raise SCADA security awareness.

The following link provides materials lists, software, and instructions on how to setup various SCADA systems. As more development occurs in our CyberVille, these will be updated to the link. With a small investment in time and money your curriculum could stand up its own CyberVille to enhance SCADA security awareness education.

### III. CONCLUSION

Creating a SCADA attack model such as CyberVille provides an inexpensive hands-on experience for helping all students become aware of the danger of cyber attacks. Using the model to highlight multi-level effects helps students consider the cascading impacts that SCADA systems could have on their security. It is our hopes that this approach creates more security mindedness for both students entering the information technology field and those will one day be users of these tools.

#### Disclaimer

The views expressed in this paper are those of the authors and do not necessarily reflect the official policy or position of the Department of the Air Force, the Department of Defense, or the U.S. Government.

### REFERENCES

- [1] (2012) U.S Department of Defense website. [Online]. Available:<http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136>
- [2] Staff of Congressman E. Markey, H. Waxman, "Electric Grid Vulnerability: Industry Responses Reveal Security Gaps," *Report to U.S. House of Representatives*, May 2013
- [3] (2013) The White House website. [Online]. Available: <http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>
- [4] Kushner, David. "The Real Story of Stuxnet," *IEEE Spectrum*, February 2013.
- [5] Lori A. Burkman, "Cyber Attack!- Lessons Learned: Aurora Attack," *Fortnightly Magazine*, January 2008.

- [6] Carlisle and Schweitzer, "Promoting Skepticism in the Security Classroom," *Proceedings of the 14th Colloquium for Information Systems Security Education*, Baltimore MD, June 2010.
- [7] (2013) NetWars: CyberCity, SANS, [Online] <http://www.sans.org/netwars/cybercity>.